2001".

Reconsideration and allowance of the above-referenced application are respectfully requested. Claims 1-35 are unchanged and remain pending in the application.

The withdrawn objection to the drawings is acknowledged with appreciation.

Claims 1-35 stand rejected under 35 USC §102(e) in view of U.S. Patent Publication No. 2003/0093563 to Young et al. This rejection is respectfully traversed.

The Final Action demonstrates a disregard of the explicit claim language. In particular, the Examiner asserts on page 2 of the Final Action that "the features upon which applicant relies (i.e., multiple secure connections) *are not recited in the rejected claim(s).*"

In fact, this limitation of multiple secure connections is explicitly recited in each of the independent claims 1, 10, 18, and 27. Claims 1 and 10 are exemplary:

1. A method in a router having at least one outbound interface, the method comprising:

establishing, on the outbound interface, ***a plurality of*** *Internet Protocol (IP)-based* ***secure connections*** with respective destinations based on receiving encrypted packets generated by a cryptographic module, *each encrypted packet successively output from the cryptographic module having a corresponding successively-unique sequence number*;

controlling supply of data packets to the cryptographic module by:

(1) *assigning,* ***for each secure connection,*** *a corresponding queuing module,*

(2) reordering, in each queuing module, *a corresponding group of the data packets* ***associated with the corresponding secure connection*** according to a determined quality of service policy and based on a corresponding assigned maximum output bandwidth for the corresponding queuing module, and

(3) outputting to the cryptographic module the group of data packets, from each corresponding queuing module according to the corresponding assigned maximum output bandwidth, for generation of the encrypted packets; and

second outputting the encrypted packets from the cryptographic module to the outbound interface for transport via their associated ***secure connections***.

10. A router comprising:

a cryptographic module configured for successively outputting *encrypted packets having respective successively-unique sequence numbers*;

an outbound interface configured for establishing ***a plurality of*** *Internet Protocol (IP)-based* ***secure connections*** with respective destinations based on receiving respective streams of the encrypted packets; and

a queue controller configured for controlling supply of data packets to the cryptographic module, *the queue controller configured for assigning, **for each secure connection**, a corresponding queuing module*, each queuing module configured for:

(1) outputting to the cryptographic module *a corresponding group of the data packets associated with the corresponding **secure connection***, and according to a corresponding assigned maximum output bandwidth for the corresponding queuing module, for generation of the corresponding stream of the encrypted packets, and

(2) reordering the corresponding group of the data packets according to a determined quality of service policy and the corresponding assigned maximum output bandwidth.

Hence, the assertion that the claims do not recite "multiple secure connections" is refuted by the explicit recital of "a plurality of Internet Protocol (IP)-based secure connections" in each of the independent claims 1, 10, 18, and 27, and demonstrates an improper disregard of the explicit claim language. Consequently, the rejection is per se improper because it fails to consider each and every claim limitation.[1]

Further, anticipation cannot be established based on a piecemeal application of the reference, where the Examiner picks and chooses isolated features of the reference in an attempt to synthesize the claimed invention.[2] In other words, it is not sufficient that a single prior art reference discloses each element that is claimed, but the reference also must disclose that the elements are arranged as in the claims under review. *In re Bond*, 15 USPQ2d 1566, 1567 (Fed. Cir. 1990) (citing *Lindemann Maschinenfabrik GmbH*).

The Examiner, however, demonstrates on page 2 of the Final Action that the rejection is based on a piecemeal evaluation of the applied reference and the claim language, without regard to the manner in which the claimed features are arranged in the claim. In particular, the Examiner fails to demonstrate that Young teaches: (1) "assigning, ***for each secure connection***, a

[1] "All words in a claim must be considered in judging the patentability of that claim against the prior art." *In re Wilson*, 424 F.2d 1382, 1385, 165 USPQ 494, 496 (CCPA 1970)."

[2] "Anticipation requires the presence in a single prior art reference disclosure of each and every element of the claimed invention, arranged as in the claim." *Lindemann Maschinenfabrik GmbH v. American Hoist & Derrick Co.*, 221 USPQ 481, 485 (Fed. Cir. 1984). "Anticipation cannot be predicated on teachings in the reference which are vague or based on conjecture." *Studiengesellschaft Kohle mbH v. Dart Industries, Inc.*, 549 F. Supp. 716, 216 USPQ 381 (D. Del. 1982), *aff'd.*, 726 F.2d 724, 220 USPQ 841 (Fed. Cir. 1984).

corresponding queuing module", or (2) ***reordering, in each queueing module***, the corresponding group of data packets associated with the corresponding secure connection, or (3) outputting to the cryptographic module the corresponding group of data packets from the corresponding queuing module according to a corresponding assigned maximum output bandwidth for the queuing module. Further, the Examiner fails to demonstrate that Young teaches "***reordering the corresponding group of data packets***" as specified in the independent claims, namely according to a determined quality of service policy and the ***corresponding assigned maximum output bandwidth***.

Rather, the Examiner asserts on page 2 of the Final Action that "Young teaches supporting encryption through software, [which] serves the function of controlling supply of data packets to a cryptographic module" and "MAND serves the function of a cryptographic module"; the Examiner also relies on paragraphs 97-98 as disclosing secure connections or tunnels.

However, the Examiner also asserts that a unique Transaction ID in paragraphs 71-72 "serves the purpose of a unique sequence number." This assertion by the Examiner is factually incorrect because Young explicitly defines the Transaction ID in paragraph 218 as being used only for MGCP protocol Voice over IP packets, and not encrypted packets.[3] Hence, the Transaction ID neither discloses nor suggests the claimed feature that "***each encrypted packet*** successively output from the cryptographic module having a corresponding successively-unique sequence number".

Further, the rejection fails to establish that Young discloses or suggests "controlling supply of data packets *to the cryptographic module* by ... assigning, ***for each secure connection***, a corresponding queuing module" as specified in claims 1 18, and 27, or a "queue controller configured for assigning, ***for each secure connection***, a corresponding queuing module" as specified in claim 10.

In particular, the Examiner asserts on page 2 of the Final Action (para. 4) that Young

[3] "[0218] Transaction ID--A transaction ID is a unique integer associated with each MGCP signaling request. The MAND modifies the WAN transaction ID to a unique LAN Transaction ID."

teaches "priority queuing and routing, and configuring the bandwidths in ¶19" and that "Secure connections or tunnels as disclosed as well in Young.

However, the claims do not simply specify "secure connections" or "priority queuing" as suggested by the Examiner, but rather explicitly require that each secure tunnel is assigned a corresponding queuing module: the rejection fails to establish that Young provides any disclosure or suggestion of the claimed ***"assigning, for each secure connection, a corresponding queuing module"***; rather, the Examiner relies on combining vague references to "priority queuing and routing" in combination with "secure connections or tunnels", without the required assignment to the plurality of secure connections of respective queuing modules. As such, the rejection fails to disclose each and every claim limitation.[4]

Further, the rejection fails to demonstrate that Young teaches the claimed ***"reordering, in each queuing module,*** a corresponding group of the data packets associated with the corresponding secure connection" as specified in claims 1, 18, and 27 (claim 10 specifies "each queuing module configured for ... reodering the corresponding group ...."). Rather, Young simply adds a marker to specify to external routers or switches in the Internet that "priority queuing" *should* be performed. Paragraph 19 of Young states:

> [0019] In one embodiment of the invention broadly described herein, packets such as voice, video and data packets, are transmitted over common network connections, such as a LAN or WAN. The packets are mapped from a public address field (such as an IP address) and port number to a private address field and port number, the mapping process typically being handled by a NAT (Network Address Translation). The packets are also prioritized, by ***marking the packets for priority queuing and routing***, and configuring the bandwidths of the WAN traffic and the voice traffic to predetermined quantities and configuring the address fields of the voice devices. The embodiment also limits the simultaneous transmission of the various packets to predetermined quantities, typically by utilizing a CAC (Client Access Control). Secure firewalls are also included in the MAND.

As apparent from the foregoing, however, Young teaches that the MAND performs only ***marking (i.e., tagging)*** the packets ***for*** priority queuing and routing, and does not disclose or

[4] See footnote 2 *supra.*

suggest the MAND actually *performing* priority queueing and routing. In particular, a traffic shaper 100 (see Fig. 3) is configured for ***marking*** packets, not priority queuing: "[v]oice and media packets can also be marked at this point for priority queuing and routing. Voice packets going out the WAN port 10 can be tagged with priorities using IP-ToS, IP Precedence, or Diffserv" (para. 51 at lines 14-17).

Further, Young teaches that the "marking" is performed to enable ***external devices*** (e.g., Internet routers and switches) to implement QoS mechanisms based on the tagged/marked packets: "There are several QoS mechanisms that can be used to prioritize real-time voice traffic over data traffic. Ethernet or IP packets can be tagged using 802.1p, IP-ToS, IP Precedence or Diffserv, ***and then prioritized in switches and routers***"(para. 9, lines 1-5).

In addition, the attached Exhibit A (pages 30, 34, and 35 of RFC 3272, "Overview and Principles of Internet Traffic Engineering") specifies that the ToS field identifies the route that should be selected by a router based on the ToS value specified within the IP packet, and that the Differentiated Services field in the IP header indicates the forwarding treatment that a packet should receive at a node.

Hence, Exhibit A demonstrates that one skilled in the art would interpret Young as teaching ***marking*** a packet (*cf.* para. 9-10, 19, and 51) so that other switches and routers can prioritize the packets.

In addition, Young teaches that incoming traffic (i.e., from the Internet 2000 of Fig. 3) is limited to avoid congesting the WAN link:

> [0009] ... Queuing schemes can be implemented in customer premise routers to prioritize outbound traffic, but more commonly the congestion problem is from web downloads and other inbound traffic. Throwing out packets at the router does not prevent a narrow WAN link from being congested from traffic coming into the link from the Internet.
>
> [0010] In order to solve these problems, the MAND supports traffic shaping in addition to tagging and queuing mechanisms. The MAND at the customer premise running traffic shaping can prioritize outbound traffic *as well as free up inbound bandwidth for higher priority voice traffic. This is done by forcing the lower priority inbound data traffic to back-off so that it does not congest the WAN link*.

See also para. 51, which specifies that the traffic shaper 100 of Fig. 3 "pushes back" incoming WAN traffic from the Internet to open up bandwidth for higher priority voice packets.[5]

Thus, Young teaches that the traffic shaper 100: (1) limits incoming traffic to free up bandwidth on the WAN link for outgoing higher priority traffic; (2) and ***marks*** outgoing IP packets (e.g., according to IP-ToS, IP Precedence or Diffserv) "for priority queuing and routing" to be performed by **subsequent switches and routers in the Internet 2000**. Further, Young teaches that a Client Access Control (CAC) limits outgoing traffic

Hence, Young fails to disclose or suggest any ***reordering*** of packets output by the MAND device at all!

Young et al. provides only vague references to IPSec encryption for VPN tunneling, without any specific description of how a specific VPN tunnel should be established. Young et al. provides no disclosure whatsoever of the claimed controlling supply of data packets ***to the cryptographic module***, but actually performs QoS congestion control after encryption has been performed.

Hence, Young et al. neither discloses nor suggests the specific features in independent claims 1, 10, 18, and 27 of controlling supply of data packets to a cryptographic module by: (1) assigning, for each of the multiple secure connections, a corresponding queuing module (queuing means in claim 27); (2) reordering, ***within the corresponding queuing module*** (queueing means), the corresponding group of data packets ***associated with the corresponding secure connection*** according to the determined quality of service policy and the corresponding assigned maximum output bandwidth ***for the corresponding queuing module***.

For these and other reasons, the §102 rejection should be withdrawn.

Applicant further traverses the Final Action as incomplete, because it does not address all

[5] "FIG. 3 shows an exemplary network system consistent with the principles of the present invention. Packets coming from the WAN 10 and LAN 30 ports first pass through the traffic shaper 100. The traffic shaper 100 can be configured to slow and "push back"-lower priority traffic coming into the WAN 10 and LAN 30 ports from the Internet 2000 to open up bandwidth for higher priority voice packets. "

material traversed. In particular, the following arguments were initially presented on pages 12-13 of the Amendment filed January 4, 2006, but were never addressed by the Examiner. (See MPEP §707.07(f) "Where the applicant traverses any rejection, the examiner should, if he or she repeats the rejection, take note of the applicant's argument and answer the substance of it.").

Paragraphs 84-87 provide no disclosure or suggestion whatsoever of "***outputting to the cryptographic module*** a corresponding group of the data packets associated with the corresponding secure connection, and according to a corresponding assigned maximum output bandwidth ***for the corresponding queuing module***; rather, paragraphs 84-87 describe Client Access Control with respect to Fig. 10, where if a voice caller cannot initiate a call during call setup due to limited capacity ("the bandwidth is not available"), the calling party is sent a "resource unavailable message" such as a "fast busy tone". Hence, Paragraphs 84-87 describe a complete denial of service!

Moreover, Young et a. describes monitoring only total (i.e., aggregate) capacity: there is no disclosure or suggestion of the claimed "assigned maximum output bandwidth for the corresponding queuing module". Paragraph 86 explicitly states that "the number of active calls is compared to the CAC active call counter 1506. If this number is exceeded then a resource unavailable message 1520 is sent 1522 to the requesting device." Further, paragraph 87 states that "the requested bandwidth is compared to the remaining bandwidth available in the CAC bandwidth counter 1510. ... If the bandwidth is not available, a resource unavailable message is sent to the requesting device."

For these and other reasons, the §102 rejection should be withdrawn.

In view of the above, it is believed this application is in condition for allowance, and such a Notice is respectfully solicited.

To the extent necessary, Applicant petitions for an extension of time under 37 C.F.R. 1.136. Please charge any shortage in fees due in connection with the filing of this paper, including any missing or insufficient fees under 37 C.F.R. 1.17(a), to Deposit Account No. 50-1130, under Order No. 10-008, and please credit any excess fees to such deposit account.

Respectfully submitted,

Leon R. Turkevich
Registration No. 34,035

Customer No. 23164
(202) 261-1059
Date: Monday, April 24, 2006
(April 23, 2006 = Sunday)

4.2.3 ToS Routing

Type-of-Service (ToS) routing involves different routes going to the same destination with selection dependent upon the ToS field of an IP packet [RFC-2474]. The ToS classes may be classified as low delay and high throughput. Each link is associated with multiple link costs and each link cost is used to compute routes for a particular ToS. A separate shortest path tree is computed for each ToS. The shortest path algorithm must be run for each ToS resulting in very expensive computation. Classical ToS-based routing is now outdated as the IP header field has been replaced by a Diffserv field. Effective traffic engineering is difficult to perform in classical ToS-based routing because each class still relies exclusively on shortest path routing which results in localization of traffic concentration within the network.

4.2.4 Equal Cost Multi-Path

Equal Cost Multi-Path (ECMP) is another technique that attempts to address the deficiency in the Shortest Path First (SPF) interior gateway routing systems [RFC-2328]. In the classical SPF algorithm, if two or more shortest paths exist to a given destination, the algorithm will choose one of them. The algorithm is modified slightly in ECMP so that if two or more equal cost shortest paths exist between two nodes, the traffic between the nodes is distributed among the multiple equal-cost paths. Traffic distribution across the equal-cost paths is usually performed in one of two ways: (1) packet-based in a round-robin fashion, or (2) flow-based using hashing on source and destination IP addresses and possibly other fields of the IP header. The first approach can easily cause out-of-order packets while the second approach is dependent upon the number and distribution of flows. Flow-based load sharing may be unpredictable in an enterprise network where the number of flows is relatively small and less heterogeneous (for example, hashing may not be uniform), but it is generally effective in core public networks where the number of flows is large and heterogeneous.

In ECMP, link costs are static and bandwidth constraints are not considered, so ECMP attempts to distribute the traffic as equally as possible among the equal-cost paths independent of the congestion status of each path. As a result, given two equal-cost paths, it is possible that one of the paths will be more congested than the other. Another drawback of ECMP is that load sharing cannot be achieved on multiple paths which have non-identical costs.

Under RSVP, the sender or source node sends a PATH message to the receiver with the same source and destination addresses as the traffic which the sender will generate. The PATH message contains: (1) a sender Tspec specifying the characteristics of the traffic, (2) a sender Template specifying the format of the traffic, and (3) an optional Adspec which is used to support the concept of one pass with advertising" (OPWA) [RFC-2205]. Every intermediate router along the path forwards the PATH Message to the next hop determined by the routing protocol. Upon receiving a PATH Message, the receiver responds with a RESV message which includes a flow descriptor used to request resource reservations. The RESV message travels to the sender or source node in the opposite direction along the path that the PATH message traversed. Every intermediate router along the path can reject or accept the reservation request of the RESV message. If the request is rejected, the rejecting router will send an error message to the receiver and the signaling process will terminate. If the request is accepted, link bandwidth and buffer space are allocated for the flow and the related flow state information is installed in the router.

One of the issues with the original RSVP specification was Scalability. This is because reservations were required for micro-flows, so that the amount of state maintained by network elements tends to increase linearly with the number of micro-flows. These issues are described in [RFC-2961].

Recently, RSVP has been modified and extended in several ways to mitigate the scaling problems. As a result, it is becoming a versatile signaling protocol for the Internet. For example, RSVP has been extended to reserve resources for aggregation of flows, to set up MPLS explicit label switched paths, and to perform other signaling functions within the Internet. There are also a number of proposals to reduce the amount of refresh messages required to maintain established RSVP sessions [RFC-2961].

A number of IETF working groups have been engaged in activities related to the RSVP protocol. These include the original RSVP working group, the MPLS working group, the Resource Allocation Protocol working group, and the Policy Framework working group.

4.5.3 Differentiated Services

The goal of the Differentiated Services (Diffserv) effort within the IETF is to devise scalable mechanisms for categorization of traffic into behavior aggregates, which ultimately allows each behavior aggregate to be treated differently, especially when there is a shortage of resources such as link bandwidth and buffer space [RFC-2475]. One of the primary motivations for the Diffserv effort was to devise alternative mechanisms for service differentiation in the Internet that mitigate the scalability issues encountered with the Intserv model.

The IETF Diffserv working group has defined a Differentiated Services field in the IP header (DS field). The DS field consists of six bits of the part of the IP header formerly known as TOS octet. The DS field is used to indicate the forwarding treatment that a packet should receive at a node [RFC-2474]. The Diffserv working group has also standardized a number of Per-Hop Behavior (PHB) groups. Using the PHBs, several classes of services can be defined using different classification, policing, shaping, and scheduling rules.

For an end-user of network services to receive Differentiated Services from its Internet Service Provider (ISP), it may be necessary for the user to have a Service Level Agreement (SLA) with the ISP. An SLA may explicitly or implicitly specify a Traffic Conditioning Agreement (TCA) which defines classifier rules as well as metering, marking, discarding, and shaping rules.

Packets are classified, and possibly policed and shaped at the ingress to a Diffserv network. When a packet traverses the boundary between different Diffserv domains, the DS field of the packet may be re-marked according to existing agreements between the domains.

Differentiated Services allows only a finite number of service classes to be indicated by the DS field. The main advantage of the Diffserv approach relative to the Intserv model is scalability. Resources are allocated on a per-class basis and the amount of state information is proportional to the number of classes rather than to the number of application flows.

It should be obvious from the previous discussion that the Diffserv model essentially deals with traffic management issues on a per hop basis. The Diffserv control model consists of a collection of micro-TE control mechanisms. Other traffic engineering capabilities, such as capacity management (including routing control), are also required in order to deliver acceptable service quality in Diffserv networks. The concept of Per Domain Behaviors has been introduced to better capture the notion of differentiated services across a complete domain [RFC-3086].

4.5.4 MPLS

MPLS is an advanced forwarding scheme which also includes extensions to conventional IP control plane protocols. MPLS extends the Internet routing model and enhances packet forwarding and path control [RFC-3031].